

# CHARACTERIZATION OF A HERMITIAN CURVE BY GALOIS POINT

SATORU FUKASAWA

**ABSTRACT.** For a plane curve, a point in the projective plane is said to be Galois when the point projection induces a Galois extension of function fields. We give a new characterization of a Fermat curve whose degree minus one is a power of  $p$  in characteristic  $p > 2$ , which is sometimes called Hermitian, by the number of Galois points lying on the curve.

## 1. INTRODUCTION

Let  $C \subset \mathbb{P}^2$  be an irreducible plane curve of degree  $d \geq 4$  over an algebraically closed field  $K$  of characteristic  $p \geq 0$  and let  $K(C)$  be the function field of  $C$ . The point projection  $\pi_P : C \dashrightarrow \mathbb{P}^1$  from a point  $P \in \mathbb{P}^2$  induces a field extension  $K(C)/\pi_P^*K(\mathbb{P}^1)$  of function fields. When the extension is Galois, we call the point  $P$  a *Galois point* for  $C$ . This notion was introduced by H. Yoshihara ([2], [14], [19]). A Galois point  $P \in \mathbb{P}^2$  is said to be inner if  $P \in C_{\text{sm}}$ , where  $C_{\text{sm}}$  is the smooth locus of  $C$ . We denote by  $\delta(C)$  the number of inner Galois points. If there exist infinitely many inner Galois points, we define as  $\delta(C) = \infty$ . Otherwise, we define as  $\delta(C) < \infty$ . It is remarkable that many classification results of algebraic varieties have been obtained in the theory of Galois point.

When  $p = 0$ , Yoshihara determined the number  $\delta(C)$  for smooth curves ([19]). Miura gave a certain inequality related to  $\delta(C)$  if  $d - 1$  is prime ([13]). In  $p > 0$ , Homma proved that  $\delta(H) = (p^e)^3 + 1$  for a Fermat curve  $H$  of degree  $p^e + 1$  ([11]), which is sometimes called Hermitian. Recently, the present author determined  $\delta(C)$  for any other smooth curve  $C$  ([4]). On the other hand, Hasegawa and the present author [5] found examples of plane curves having infinitely many Galois points and classified them. Then, we have a natural question: *When  $\delta(C)$  is finite, what is the maximal number  $\delta(C)$ ?* The purpose of this paper is to answer this question, which leads to a new characterization of a Hermitian curve.

---

2000 *Mathematics Subject Classification.* Primary 14H50; Secondary 12F10.

*Key words and phrases.* Galois point, plane curve, positive characteristic, Hermitian curve.

**Theorem.** *Let  $C \subset \mathbb{P}^2$  be an irreducible plane curve of degree  $d \geq 4$  over an algebraically closed field  $K$  of characteristic  $p \neq 2$ . If  $\delta(C) < \infty$ , then  $\delta(C) \leq (d-1)^3 + 1$ . Furthermore,  $\delta(C) = (d-1)^3 + 1$  if and only if  $p > 0$ ,  $d-1$  is a power of  $p$ , and  $C$  is projectively equivalent to a Fermat curve.*

## 2. PRELIMINARIES

Let  $(X : Y : Z)$  be a system of homogeneous coordinates of the projective plane  $\mathbb{P}^2$  and let  $C \subset \mathbb{P}^2$  be an irreducible plane curve of degree  $d \geq 4$ . We denote by  $C_{\text{sm}}$  the smooth locus of  $C$  and by  $\text{Sing}(C)$  the singular locus of  $C$ . If  $P \in C_{\text{sm}}$ , we denote by  $T_P C \subset \mathbb{P}^2$  the (projective) tangent line at  $P$ . For a projective line  $l \subset \mathbb{P}^2$  and a point  $P \in C \cap l$ , we denote by  $I_P(C, l)$  the intersection multiplicity of  $C$  and  $l$  at  $P$ .

A tangent line at a singular point  $Q \in \text{Sing}(C)$  is defined as follows. Let  $f(x, y)$  be the defining polynomial of  $C$  in the affine plane defined by  $Z \neq 0$ , and let  $Q = (0 : 0 : 1)$ . We can write  $f = f_m + f_{m+1} + \cdots + f_d$ , where  $f_i$  is the  $i$ -th homogeneous component. A tangent line at  $Q$  is the line defined by an irreducible component of  $f_m$ . Therefore, a line  $l$  passing through  $Q$  is a tangent line at  $Q$  if and only if  $I_Q(C, l) > m$ .

Let  $r : \hat{C} \rightarrow C$  be the normalization and let  $g$  (or  $g_C$ ) be the genus of  $\hat{C}$ . We denote by  $\overline{PR}$  the line passing through points  $P$  and  $R$  when  $R \neq P$ , and by  $\pi_P : C \dashrightarrow \mathbb{P}^1; R \mapsto \overline{PR}$  the point projection from a point  $P \in \mathbb{P}^2$ . We write  $\hat{\pi}_P = \pi_P \circ r$ . We denote by  $e_{\hat{R}}$  the ramification index of  $\hat{\pi}_P$  at  $\hat{R} \in \hat{C}$ . If  $R = r(\hat{R}) \in C_{\text{sm}}$ , then we denote  $e_{\hat{R}}$  also by  $e_R$ . It is not difficult to check the following.

**Lemma 1.** *Let  $P \in \mathbb{P}^2$  and let  $\hat{R} \in \hat{C}$  with  $r(\hat{R}) = R \neq P$ . Then for  $\hat{\pi}_P$  we have the following.*

- (1) *If  $P \in C_{\text{sm}}$ , then  $e_P = I_P(C, T_P C) - 1$ .*
- (2) *If  $h$  be a linear polynomial defining  $\overline{RP}$ , then  $e_{\hat{R}} = \text{ord}_{\hat{R}} r^* h$ . In particular, if  $R$  is smooth, then  $e_R = I_R(C, \overline{PR})$ .*

Let  $\check{\mathbb{P}}^2$  be the dual projective plane, which parameterizes lines on  $\mathbb{P}^2$ . The dual map  $\gamma : C_{\text{sm}} \rightarrow \check{\mathbb{P}}^2$  of  $C$  is a rational map which assigns a smooth point  $P \in C_{\text{sm}}$  to the tangent line  $T_P C \in \check{\mathbb{P}}^2$  at  $P$ , and the dual curve  $C^* \subset \check{\mathbb{P}}^2$  is the closure of the image of  $\gamma$ . We denote by  $s(\gamma)$  the separable degree of the field extension  $K(C)/\gamma^* K(C^*)$ , which is induced from the dual map  $\gamma$  of  $C$  onto  $C^*$ , by  $q(\gamma)$  the inseparable degree, and by  $M(C)$  the generic order of contact (i.e.  $I_P(C, T_P C) =$

$M(C)$  for a general point  $P \in C$ ), throughout this paper. If the dual map  $\gamma$  is separable onto  $C^*$ , then  $s(\gamma) = 1$  and  $M(C) = 2$  (see, for example, [15, Proposition 1.5]). If the dual map  $\gamma$  of  $C$  is not separable, then it follows from a theorem of Hefez-Kleiman ([8, (3.4)]) that  $M(C) = q(\gamma)$ . Using this theorem and Bézout's theorem, we find that  $d \geq s(\gamma)q(\gamma)$ .

The order sequence of the morphism  $r : \hat{C} \rightarrow \mathbb{P}^2$  is  $\{0, 1, M(C)\}$  (see [9, Ch. 7], [18]). If  $\hat{R} \in \hat{C}$  is a non-singular branch, i.e. there exists a line defined by  $h = 0$  with  $\text{ord}_{\hat{R}} r^* h = 1$ , then there exists a unique tangent line at  $R = r(\hat{R})$  defined by  $h_{\hat{R}} = 0$  such that  $\text{ord}_{\hat{R}} r^* h_{\hat{R}} \geq M(C)$ . We denote by  $T_{\hat{R}} C \subset \mathbb{P}^2$  this tangent line, and by  $\nu_{\hat{R}}$  the order  $\text{ord}_{\hat{R}} r^* h_{\hat{R}}$  of the tangent line  $h_{\hat{R}} = 0$  at  $\hat{R}$ . If  $\nu_{\hat{R}} - M(C) > 0$ , then we call the point  $\hat{R}$  (or  $R = r(\hat{R})$  if  $R \in C_{\text{sm}}$ ) a *flex*. We denote by  $\hat{C}_0 \subset \hat{C}$  the set of all non-singular branches and by  $F(\hat{C}) \subset \hat{C}_0$  the set of all flexes. We recall the following (see [18, Theorem 1.5]).

**Fact 1** (Count of flexes). *We have*

$$\sum_{\hat{R} \in \hat{C}_0} (\nu_{\hat{R}} - M(C)) \leq (M(C) + 1)(2g - 2) + 3d.$$

We also recall Plücker formula. (This version is obtained easily from considering the projection from a general point of  $\mathbb{P}^2$  and the number of singular points of  $C^*$ , since a general point of  $\mathbb{P}^2$  corresponds to a general line in  $\check{\mathbb{P}}^2$ . See also [16].)

**Fact 2** (Plücker formula). *Let  $d^*$  be the degree of the dual curve  $C^*$ . Then,*

$$d^* \leq 2g - 2 + 2d.$$

*If  $s(\gamma) = 1$ , then the number of multiple tangent lines (i.e. lines  $L$  such that there exist two distinct points  $\hat{R}_1, \hat{R}_2 \in \hat{C}_0$  with  $L = T_{\hat{R}_1} C = T_{\hat{R}_2} C$ ) is at most*

$$\frac{(d^* - 1)(d^* - 2)}{2} \leq \frac{(2g - 2 + 2d - 1)(2g - 2 + 2d - 2)}{2}.$$

We recall the definition of strangeness. If there exists a point  $Q \in \mathbb{P}^2$  such that almost all tangent lines of  $C$  pass through  $Q$ , then  $C$  is said to be *strange* and  $Q$  is called a *strange center* (see [1], [12]). It is easily checked that a strange center is unique for a strange curve. Using Lemma 1, we find that the projection  $\hat{\pi}_Q$  from a point  $Q$  is not separable if and only if  $C$  is strange and  $Q$  is the strange center. If  $C$  is strange, then we can identify the dual map  $\gamma$  with the projection  $\pi_Q$  from the strange center  $Q$ .

We denote by  $\Delta \subset \hat{C}$  the set of all points  $\hat{P} \in \hat{C}$  such that  $r(\hat{P}) \in C$  is smooth and Galois with respect to a plane curve  $C \subset \mathbb{P}^2$ . We denote by  $G_P$  the group of birational maps from  $C$  to itself corresponding to the Galois group  $\text{Gal}(K(C)/\pi_P^*K(\mathbb{P}^1))$  when  $P$  is Galois. We find easily that the group  $G_P$  is isomorphic to a subgroup of the automorphism group  $\text{Aut}(\hat{C})$  of  $\hat{C}$ . Frequently, we identify  $G_P$  with the subgroup. If a Galois covering  $\theta : C \rightarrow C'$  between smooth curves is given, then the Galois group  $G$  acts on  $C$  naturally. We denote by  $G(P)$  the stabilizer subgroup of  $P$  and by  $e_P$  the ramification index at  $P$ . The following fact is useful to find Galois points (see [17, III. 7.1, 7.2 and 8.2]).

**Fact 3.** *Let  $\theta : C \rightarrow C'$  be a Galois covering of degree  $d$  with a Galois group  $G$ . Then we have the following.*

- (1) *The order of  $G(P)$  is equal to  $e_P$  at  $P$  for any point  $P \in C$ .*
- (2) *If  $\theta(P) = \theta(Q)$ , then  $e_P = e_Q$ .*
- (3) *The index  $e_P$  divides the degree  $d$ .*

By using Lemma 1 and Fact 3, we have the following.

**Lemma 2.** *Let  $P_1, P_2 \in C_{\text{sm}}$  be two distinct Galois points and let  $h$  be a defining polynomial of the line  $\overline{P_1P_2}$ . Then,  $\text{ord}_{\hat{R}}r^*h = 1$  for any  $\hat{R} \in \hat{C}$  with  $R = r(\hat{R}) \in \overline{P_1P_2}$  (maybe  $R = P_1$  or  $P_2$ ).*

*Proof.* Assume that  $R = P_2$  and  $\text{ord}_{\hat{R}}r^*h \geq 2$ . It follows from Lemma 1 that  $e_{P_2} = I_{P_2}(C, \overline{P_1P_2}) - 1$  for a projection  $\hat{\pi}_{P_2}$ . Then, by Fact 3(2) and Lemma 1,  $I_{P_1}(C, \overline{P_1P_2}) = I_{P_2}(C, \overline{P_1P_2}) - 1$ . If  $I_{P_1}(C, \overline{P_1P_2}) \geq 2$ , then, for  $\hat{\pi}_{P_1}$ ,  $e_{P_1} = I_{P_1}(C, \overline{P_1P_2}) - 1 \geq 1$  and  $e_{P_1} = e_{P_2} = I_{P_2}(C, \overline{P_1P_2})$ , by Lemma 1 and Fact 3(2). Then, we have  $I_{P_2}(C, \overline{P_1P_2}) - 2 = I_{P_2}(C, \overline{P_1P_2})$ . This is a contradiction. Therefore,  $I_{P_1}(C, \overline{P_1P_2}) = 1$  and  $I_{P_2}(C, \overline{P_1P_2}) = 2$ . Since  $d > 3$ , there exist a point  $\hat{R}_0 \in \hat{C}$  such that  $R_0 = r(\hat{R}_0) \in \overline{P_1P_2}$  and  $R_0 \neq P_1, P_2$ . By Fact 3(2), we have  $e_{\hat{R}_0} = 2$  for  $\hat{\pi}_{P_1}$  and  $e_{\hat{R}_0} = 1$  for  $\hat{\pi}_{P_2}$ . This is a contradiction, because  $e_{\hat{R}} = \text{ord}_{\hat{R}}r^*h$  for each case, by Lemma 1.

Assume that  $R \neq P_1, P_2$  and  $\text{ord}_{\hat{R}}r^*h \geq 2$ . Then, by considering  $\hat{\pi}_{P_1}$  and Lemma 1 and Fact 3(2),  $I_{P_2}(C, \overline{P_1P_2}) = \text{ord}_{\hat{R}}r^*h$ . Then, by considering  $\hat{\pi}_{P_2}$  and Lemma 1 and Fact 3(2),  $I_{P_2}(C, \overline{P_1P_2}) - 1 = \text{ord}_{\hat{R}}r^*h$ . We have  $I_{P_2}(C, \overline{P_1P_2}) = I_{P_2}(C, \overline{P_1P_2}) - 1$ . This is a contradiction.  $\square$

Finally in this section, we mention properties of Galois covering between rational curves.

**Lemma 3.** *Let  $\theta : \mathbb{P}^1 \rightarrow \mathbb{P}^1$  be a Galois covering of degree  $d \geq 3$  with a Galois group  $G$ . Then we have the following.*

- (1) *Any automorphism  $\sigma \in G \setminus \{1\}$  fixes some point.*
- (2) *If  $P$  is a ramification point and the fiber  $\theta^{-1}(\theta(P))$  consists of at least two points, then there exists a ramification point  $P'$  with  $\theta(P') \neq \theta(P)$ .*
- (3) *If  $\theta$  is ramified only at  $P$  and  $e_P = d$ , then  $p > 0$  and  $d$  is a power of  $p$ .*
- (4) *If  $p > 0$ ,  $d$  is a power of  $p$  and the index  $e_P$  at a point  $P$  is equal to  $d$ , then  $P$  is a unique ramification point. If  $P = (1 : 0)$ , then any element  $\sigma \in G$  is represented by a matrix*

$$A_\sigma = \begin{pmatrix} 1 & a(\sigma) \\ 0 & 1 \end{pmatrix}$$

*for some  $a(\sigma) \in K$ . Furthermore, the set  $\{a(\sigma) | \sigma \in G\} \subset K$  forms an additive subgroup.*

*Proof.* Note that any automorphism of  $\mathbb{P}^1$  is represented by a matrix  $A_\sigma$ . This implies the assertion (1).

We consider the assertion (2). We assume that  $\theta^{-1}(\theta(P)) = \{P_1, P_2, \dots, P_s\}$  with  $s \geq 2$ . Then, it follows from Fact 3(1)(2) that the order of  $G(P_i)$  is equal to the one of  $G(P_j)$  for any  $i, j$ . Since  $G(P_i) \cap G(P_j)$  is not empty as a set,  $\bigcup_i G(P_i) \neq G$  as a set by considering the order. Let  $\tau \in G \setminus (\bigcup_i G(P_i))$ . By the assertion (1), there is a fixed point of  $P'$  by  $\tau$ . It follows from Fact 3(1) that  $P'$  is a ramification point of  $\theta$ . Then,  $\theta(P') \neq \theta(P)$  because  $\tau \notin \bigcup_i G(P_i)$ .

We consider the assertion (3). We may assume that  $P = (1 : 0)$ . Let  $e_P = ql$ , where  $q$  is a power of  $p$  and  $l$  is not divisible by  $p$ . Let  $\sigma \in G(P)$  be any element. Then,  $\sigma$  is represented by a matrix

$$A_\sigma = \begin{pmatrix} \zeta & a \\ 0 & 1 \end{pmatrix}$$

as an automorphism of  $\mathbb{P}^1$ , where  $\zeta$  is an  $l$ -th root of unity and  $a \in K$ , because  $\sigma(P) = P$  and  $\sigma^{ql} = 1$ . If  $\zeta \neq 1$ , then we find that  $\sigma$  has two fixed points, by direct computations. Therefore,  $\zeta = 1$  by our assumption. Then, any element of  $G(P) \setminus \{1\}$  is of order  $p$ , by direct computations. If  $l > 1$  then there exists an element whose order is not divisible by  $p$ , by Sylow's theorem. This is a contradiction. Therefore,  $l = 1$ .

We consider the assertion (4). We may assume that  $P = (1 : 0)$ . Let  $e_P = q$ , where  $q$  is a power of  $p$ . It follows from Fact 3(1) that the order of  $G(P)$  is equal to  $q$ . Let  $\sigma \in G(P)$ . Then, by direct computations,  $\sigma$  is represented by a matrix

$$A_\sigma = \begin{pmatrix} 1 & a(\sigma) \\ 0 & 1 \end{pmatrix}$$

as an automorphism of  $\mathbb{P}^1$ , where  $a(\sigma) \in K$ , because  $\sigma(P) = P$  and  $\sigma^q = 1$ . Then, it is not difficult to check that  $\sigma$  fixes only a point  $P$  and the subset  $\{a(\sigma) | \sigma \in G\} \subset K$  forms an additive subgroup.  $\square$

### 3. PROOF

If  $p > 0$ ,  $d - 1$  is a power of  $p$  and  $C$  is projectively equivalent to a Fermat curve of degree  $d$ , then it follows from a result of Homma [11] that  $\delta(C) = (d - 1)^3 + 1$ .

Throughout this section, we assume that  $(d - 1)^3 + 1 = (2 \times ((d - 1)(d - 2)/2) - 2)d + 3d \leq \delta(C) < \infty$ . Let  $\lambda(C)$  be the cardinality of  $\Delta \setminus F(\hat{C})$  and let  $\mu(C) = (d - 1)^3 + 1 - \{(2g - 2)(M(C) + 1) + 3d\}$ . Then,  $\lambda(C) \geq \mu(C)$ , and  $\mu(C) > 0$  if  $g < (d - 1)(d - 2)/2$  or  $M(C) < d - 1$ . Since the present author proved that  $\delta(C) = 0$  or  $\infty$  if  $d = M(C)$  in [3], we may assume that  $d > M(C)$ . It follows from a result of the author [4] for smooth curves (or a generalization of Pardini's theorem by Hefez [7] and Homma [10]) that  $\mu(C) = 0$  only if  $p > 0$ ,  $d - 1$  is a power of  $p$ , and  $C$  is a Fermat curve of degree  $d$ . Therefore, we may assume that  $\mu(C) > 0$ .

(I) *The case where there exists a singular point  $Q$  with multiplicity  $d - 1$ .* Then,  $\hat{C}$  is rational and  $Q$  is a unique singular point. It follows from Bézout's theorem that the tangent line  $T_P C$  at any smooth point  $P$  does not contain  $Q$ . Since  $d > M(C)$ ,  $T_P C$  intersects some smooth point  $R$ .

(I-1) Assume that  $M(C) \geq 3$ . Since  $\lambda(C) > 0$ , there exists a smooth point  $P$  which is Galois and  $I_P(C, T_P C) = M(C)$ . Then, it follows from Lemma 1 and Fact 3(2) that  $I_R(C, T_R C) = M(C) - 1 \geq 2$ . This is a contradiction to the order sequence  $\{0, 1, M(C)\}$ .

(I-2) Assume that  $M(C) = 2$ . Note that for any  $R \in C_{\text{sm}}$ ,  $T_R C$  contains at most one inner Galois point by Lemma 2. Therefore, we have at least  $\mu(C)$  Galois points  $P$  which do not lie on any tangent lines at flexes.

(I-2-1) Assume that  $s(\gamma) = 1$ . Let  $P \in r(\Delta) \setminus \bigcup_{\hat{R} \in F(\hat{C})} T_{\hat{R}} C$ . Assume that the fiber  $r^{-1}(Q)$  contains two or more points. It follows from Lemma 3(2) that there exists a ramification point  $\hat{R} \in \hat{C}$  with  $R = r(\hat{R}) \neq Q$  for  $\hat{\pi}_P$ . It follows from Lemma

1 and Fact 3(4) that  $P \in T_R C$  and  $I_{P_0}(C, T_R C) = 2$  for any point  $P_0 \in C \cap T_R C$  with  $P_0 \neq P$ , for each  $P \in r(\Delta) \setminus \bigcup_{\hat{R} \in F(\hat{C})} T_{\hat{R}} C$ . Therefore, we have at least  $\mu(C)$  multiple tangent lines. It follows from Fact 2 that

$$\mu(C) \leq \frac{(d_0 - 1)(d_0 - 2)}{2},$$

where  $d_0 = 2g - 2 + 2d = 2d - 2$ . Since  $\mu(C) = d^3 - 3d^2 + 6$ , we have an inequality

$$d^3 - 3d^2 + 6 \leq 2d^2 - 7d + 6.$$

Then, we have  $g_1(d) := d^3 - 5d^2 + 7d \leq 0$ . Since  $g_1(4) = 12$ , this is a contradiction.

Assume that the fiber  $r^{-1}(Q)$  consists of a unique point  $\hat{Q}$ . Then, by Fact 3(2),  $\hat{\pi}_P$  is ramified at  $\hat{Q}$  with index  $d - 1$ . It follows from Lemma 3(3)(4) that there exists a Galois point  $P$  such that  $\hat{\pi}_P$  is ramified only at  $\hat{Q}$  if and only if  $p > 0$  and  $d - 1$  is a power of  $p$ . If  $\hat{\pi}_P$  has another ramification point for any  $P \in r(\Delta) \setminus \bigcup_{\hat{R} \in F(\hat{C})} T_{\hat{R}} C$ , then, similarly to the discussion above, there is a contradiction. Therefore,  $d - 1$  is a power of  $p$  and  $\hat{Q}$  is a unique ramification point of  $\hat{\pi}_P$  for any  $P \in r(\Delta) \setminus \bigcup_{\hat{R} \in F(\hat{C})} T_{\hat{R}} C$ , by Lemma 3(4) again. Let the normalization  $r(s : t) = (\phi_0(s, t) : \phi_1(s, t) : \phi_2(s, t))$ , where  $\phi_i$  is a homogeneous polynomial of degree  $d$  in variables  $s, t$  for  $i = 0, 1, 2$ . For a suitable system of coordinates, we may assume that  $Q = (1 : 0 : 0)$  and a line  $Z = 0$  is a tangent line at  $Q$ . Since a solution of  $\phi_2(s, t) = 0$  is unique, we may assume that  $\phi_2(s, t) = t^d$ . Then,  $\hat{Q} = (1 : 0)$ . Since the projection  $\hat{\pi}_Q$  from  $Q$  is given by  $(s : 1) \mapsto (\phi_1(s, 1) : 1)$  and this is birational,  $\phi_1(s, 1)$  is of degree one. Therefore, we may assume that  $\phi_1(s, t) = st^{d-1}$ . We may also assume that  $P = (0 : 0 : 1)$ . Then,  $\phi_0(s, 1) = \sum_{i=1}^d a_i s^i$  for some  $a_i \in K$ . The projection  $\hat{\pi}_P$  from  $P$  is given by  $(\sum_{i=1}^d a_i s^i : s) = (\sum_{i=1}^d a_i s^{i-1} : 1)$ . Since  $\hat{\pi}_P$  gives a Galois covering and  $\sigma(\hat{Q}) = \hat{Q}$  for any  $\sigma \in G_P$ , it follows from Lemma 3(4) and [6, Proposition 1.1.5 and Theorem 1.2.1] that  $a_i = 0$  if  $i - 1$  is not a power of  $p$ . Let  $P_2 = (\phi_0(\alpha, 1) : \alpha : 1)$  be inner Galois. Then, the projection  $\hat{\pi}_{P_2}$  is given by  $(\phi_0(s, 1) - \phi_0(\alpha) : s - \alpha)$ . Let  $u := s - \alpha$ . Then,  $\hat{\pi}_{P_2} = (\phi_0(u + \alpha, 1) - \phi_0(\alpha) : u) = (\sum_{i=0}^e a_i \{(u + \alpha)^{p^i+1} - \alpha^{p^i+1}\} : u)$ . Note that  $\{(u + \alpha)^{p^i+1} - \alpha^{p^i+1}\}/u = u^{p^i} + \alpha u^{p^i-1} + \alpha^{p^i}$ . By considering the differential of this polynomial, if  $\alpha \neq 0$ , then  $\hat{\pi}_{P_2}$  is ramified other points than  $\hat{Q}$ . This is a contradiction to the uniqueness of the ramification point.

(I-2-2) Assume that  $s(\gamma) \geq 2$ . Then,  $q(\gamma) \geq 2$  and the number of tangent lines whose contact points are strictly less than  $s(\gamma)$  is at most

$$2g_C - 2 - s(\gamma)(2g_{C^*} - 2) = -2 + 2s(\gamma) \leq -2 + 2(d/2) = d - 2$$

by Riemann-Hurwitz formula. Since  $\mu(C) - (d - 2) = d^3 - 3d^2 - d + 8 > 0$ , there exist an inner Galois point  $P$  and a smooth point  $R \in C_{\text{sm}}$  with  $R \neq P$  such that  $T_PC = T_RC$  and  $I_P(C, T_PC) = I_R(C, T_RC) = 2$ . By Lemma 1 and Fact 3(4), this is a contradiction.

(II) *The case where there exists NO singular point with multiplicity  $d - 1$ .* Firstly, we prove that  $\hat{C}_0 = \hat{C}$ . Let  $Q$  be a singular point with multiplicity  $m \leq d - 2$ . Note that the number of tangent line at  $Q$  is at most  $m$ .

Assume that  $Q$  is not a strange center. We prove that any point  $\hat{R} \in \hat{C}$  with  $r(\hat{R}) = Q$  is a non-singular branch. If there exists a line containing  $Q$  and two Galois points, then we have this assertion by Lemma 2. Therefore, we consider the case where any line containing  $Q$  has at most one inner Galois point. If we consider the projection  $\hat{\pi}_Q$  from  $Q$ , then the number of ramification points is at most  $2g - 2 + 2(d - 2) \leq d^2 - d - 4$ . Since  $\delta(C) \geq (d - 1)^3 + 1$ , there exist a Galois point  $P$  and a point  $\hat{R} \in \hat{C}$  with  $R = r(\hat{R}) \neq P, Q$  such that  $\text{ord}_{\hat{R}} r^*h = 1$ , where  $h$  is a defining polynomial of the line  $\overline{PR}$ , by Lemma 1. It follows from Fact 3(2) that any point  $\hat{R}$  in the fiber  $r^{-1}(Q)$  is a non-singular branch.

We prove that  $Q$  is not a strange center. If there exists a line containing  $Q$  and two Galois points, then we have this assertion by Lemma 2. Therefore, we consider the case where any line containing  $Q$  has at most one inner Galois point. Assume that  $Q$  is a strange center. If we consider the projection  $\hat{\pi}_Q$  from  $Q$ , then the number of ramification points of the separable closure of  $K(C)/\hat{\pi}_Q^*K(\mathbb{P}^1)$  is at most  $2g - 2 + 2(d - 2) \leq d^2 - d - 4$ . Since  $\delta(C) \geq (d - 1)^3 + 1$ , there exist a Galois point  $P$  such that  $I_P(C, \overline{PQ}) = M(C)$ . Since any point  $\hat{R}$  with  $r(\hat{R}) \neq Q$  is a non-singular branch by discussions above,  $Q \in T_{\hat{R}}C$  for any point  $\hat{R}$  with  $r(\hat{R}) \neq Q$ . Therefore, the projection  $\hat{\pi}_P$  is ramified only at points in a line  $\overline{PQ}$ . Since the ramification index at  $P$  for  $\hat{\pi}_P$  is equal to  $M(C) - 1$  by Lemma 1, there exist only tame ramification points for  $\hat{\pi}_P$ , by Fact 3(2). By Riemann-Hurwitz formula, this is a contradiction.

(II-1) Assume that  $M(C) \geq 3$ . Since  $\lambda(C) > 0$ , there exists a Galois point  $P \in C_{\text{sm}}$  such that  $I_P(C, T_PC) = M(C)$ . Since  $d > M(C)$ , there exists a point



$R \in C \cap T_P C$ . Then, the ramification index  $e_{\hat{R}} = M(C) - 1 \geq 2$  at  $\hat{R}$  for  $\hat{\pi}_P$ , where  $\hat{R} \in \hat{C}$  with  $r(\hat{R}) = R$ . This is a contradiction to the order sequence  $\{0, 1, M(C)\}$ .

(II-2) Assume that  $M(C) = 2$ . Note that for any  $\hat{R} \in \hat{C}$ ,  $T_{\hat{R}} C$  contains at most one inner Galois points by Lemma 2. Therefore, we have at least  $\mu(C)$  Galois points  $P$  which are not flexes such that there exist no flex  $\hat{R}$  with  $P \in T_{\hat{R}} C$ . Let  $\hat{P} \in \Delta \setminus r^{-1}(\bigcup_{\hat{R} \in F(\hat{C})} T_{\hat{R}} C)$  and  $P = r(\hat{P})$ . It follows from Riemann-Hurwitz formula that  $\hat{\pi}_P$  is ramified at some point  $\hat{R} \in \hat{C}$ . It follows from Lemma 1 and Fact 3(2) that  $P \in T_{\hat{R}} C$  and the order of  $T_{\hat{R}} C$  at  $\hat{P}_0$  is equal to 2, for each  $\hat{P} \in \Delta \setminus r^{-1}(\bigcup_{\hat{R} \in F(\hat{C})} T_{\hat{R}} C)$ , a ramification point  $\hat{R}$  and  $\hat{P}_0 \in r^{-1}(C \cap T_{\hat{R}} C)$  with  $\hat{P}_0 \neq \hat{P}$ . Therefore,  $d - 1$  should be even, by Fact 3(3). Let  $n(P)$  be the number of multiple tangent lines for such a Galois point  $P$ .

(II-2-1) Assume that  $p \neq 2$ . Then,  $s(\gamma) = 1$  and  $q(\gamma) = 1$ . Since  $\hat{\pi}_P$  has only tame ramifications, it follows from Riemann-Hurwitz formula that

$$2g - 2 = -2(d - 1) + \frac{d - 1}{2} \times n(P).$$

By Lemma 2, we have at least  $\mu(C) \times n(P)$  multiple tangents. It follows from Fact 2 that

$$\mu(C) \times n(P) \leq \frac{(d_0 - 1)(d_0 - 2)}{2},$$

where  $d_0 = 2g - 2 + 2d$ . Since  $\mu(C) \geq d^3 - 6d^2 + 9d$  and  $d_0 \leq d^2 - d$ , we have an inequality

$$(d^3 - 6d^2 + 9d) \times \frac{2}{d - 1} \leq \frac{(d_0 - 1)(d_0 - 2)}{2(d_0 - 2)} \leq \frac{d^2 - d - 1}{2}.$$

Then, we have  $g_2(d) := 3d^3 - 22d^2 + 36d - 1 \leq 0$ . Since  $g_2(5) = 4$  and  $d - 1$  is even, this is a contradiction.

(II-2-2) Assume that  $p = 2$ . Then,  $q(\gamma) = 2$ . If  $s(\gamma) \geq 2$ , then the number of tangent lines whose contact points are strictly less than  $s(\gamma)$  is at most

$$2g_C - 2 - s(\gamma)(2g_{C^*} - 2) \leq 2g_C - 2 + (d/2) \times 2 < d^2 - 2d$$

by Riemann-Hurwitz formula. Since any tangent line contains at most one inner Galois point by Lemma 2 and  $\mu(C) - (d^2 - 2d) \geq d^3 - 7d^2 + 11d > 0$  if  $d \geq 5$ , there exist an inner Galois point  $P$  and a point  $\hat{R} \in \hat{C}$  with  $R = r(\hat{R}) \neq P$  such that  $T_P C = T_{\hat{R}} C$  and  $I_P(C, T_P C) = \nu_{\hat{R}} = 2$ . Considering the projection  $\hat{\pi}_P$  and Lemma 1 and Fact 3(2), this is a contradiction. Therefore,  $s(\gamma) = 1$ .

By the above arguments, we have the Theorem and the following in  $p = 2$ .

**Proposition.** *Assume that  $p = 2$ ,  $\delta(C) \geq (d - 1)^3 + 1$  and  $C$  is not projectively equivalent to a Hermitian curve. Then, we have the following.*

- (1)  $d$  is odd,  $M(C) = q(\gamma) = 2$  and  $s(\gamma) = 1$ .
- (2) There exists no singular point with multiplicity  $d - 1$ .
- (3) For any point  $\hat{R} \in \hat{C}$ , there exist a line in  $\mathbb{P}^2$  defined by  $h = 0$  around  $r(\hat{R})$  such that  $\text{ord}_{\hat{R}} r^*h = 1$ .

### Acknowledgements

The author was partially supported by Grant-in-Aid for Young Scientists (B) (22740001), JSPS, Japan.

### REFERENCES

- [1] V. Bayer and A. Hefez, Strange curves, *Comm. Algebra* **19** (1991), 3041–3059.
- [2] S. Fukasawa, Galois points for a plane curve in arbitrary characteristic, *Geom. Dedicata* **139** (2009), 211–218.
- [3] S. Fukasawa, Galois points for a non-reflexive plane curve of low degree, preprint.
- [4] S. Fukasawa, Complete determination of the number of Galois points for a smooth plane curve, preprint, arXiv:1011.3648.
- [5] S. Fukasawa and T. Hasegawa, Singular plane curves with infinitely many Galois points, *J. Algebra* **323** (2010), 10–13.
- [6] D. Goss, *Basic Structures of Function Field Arithmetic*, Springer, Berlin (1996).
- [7] A. Hefez, Non-reflexive curves, *Compositio Math.* **69** (1989), 3–35.
- [8] A. Hefez and S. Kleiman, Notes on the duality of projective varieties, “Geometry Today,” *Prog. Math.*, vol 60, Birkhäuser, Boston, 1985, pp. 143–183.
- [9] J. W. P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic Curves over a Finite Field*, Princeton Univ. Press (2008).
- [10] M. Homma, A souped-up version of Pardini’s theorem and its application to funny curves, *Compositio Math.* **71** (1989), 295–302.
- [11] M. Homma, Galois points for a Hermitian curve, *Comm. Algebra* **34** (2006), 4503–4511.
- [12] S. Kleiman, Tangency and duality, in “Proc. 1984 Vancouver Conf. in Algebraic Geometry,” *CMS Conf. Proc.* **6**, Amer. Math. Soc. (1986), pp. 163–226.
- [13] K. Miura, Galois points on singular plane quartic curves, *J. Algebra* **287** (2005), 283–293.
- [14] K. Miura and H. Yoshihara, Field theory for function fields of plane quartic curves, *J. Algebra* **226** (2000), 283–294.
- [15] R. Pardini, Some remarks on plane curves over fields of finite characteristic, *Compositio Math.* **60** (1986), 3–17.
- [16] R. Piene, Numerical characters of a curve in projective  $n$ -space, In: *Real and Complex Singularities*, Oslo 1976, pp. 475–495.

- [17] H. Stichtenoth, Algebraic Function Fields and Codes, Universitext, Springer-Verlag, Berlin (1993).
- [18] K. O. Stöhr and J. F. Voloch, Weierstrass points and curves over finite fields, Proc. London Math. Soc. (3) **52** (1986), 1–19.
- [19] H. Yoshihara, Function field theory of plane curves by dual curves, J. Algebra **239** (2001), 340–355.

DEPARTMENT OF MATHEMATICAL SCIENCES, FACULTY OF SCIENCE, YAMAGATA UNIVERSITY,  
KOJIRAKAWA-MACHI 1-4-12, YAMAGATA 990-8560, JAPAN

*E-mail address:* `s.fukasawa@sci.kj.yamagata-u.ac.jp`